National Aeronautics and
Space Administration

Headquarters
Washington, DC 20546-0001

APR 28 2008

Reply to Attn of: **Office of the Chief Information Officer**

TO: Office of the Inspector General, Office of Audits

FROM: Deputy Chief Information Officer for IT Security

SUBJECT: Decision to dispose IT Security Material Weakness

SUMMARY

The Office of the Chief Information Officer (OCIO), having shown demonstrable commitment to improving the security posture of the Agency through the execution of enterprise infrastructure improvements and progress against the Information Technology (IT) security corrective action plan (CAP); and by adequately meeting the requirements of the Federal Information Security Management Act (FISMA), is of the opinion that the IT security material weakness (MW) is disposed and makes declaration that the Agency's IT security posture be classified as other weakness (OW) as defined by internal controls deficiencies classification.

BACKGROUND

On October 19th, 2006 after a lengthy agency-wide programmatic review of IT security and based upon the recommendation of the Deputy CIO for IT Security and with concurrence from the Office of the Inspector General (OIG), the IT security posture at NASA was classified as a MW. The identification of deficiencies and associated root causes served as the requirement for the immediate development and subsequent execution of a mitigation strategy in the form of the CAP.

Ancillary and complementary to the CAP is the execution of the OCIO enterprise infrastructure integration initiatives, which serve as the underpinning to improving the Agency's IT security posture by 1) defining the network perimeter, 2) consolidating network management, establish network visibility of IT assets and consolidate Agency security monitoring and management, 3) enable cross center collaboration and strengthen user authorization, 4) make NASA's information easier to discover and access, 5) migrate Centers to appropriate managed and secure data centers, and 6) standardize and consolidate the management of end-user devices.

Finally, the completion of the certification and accreditation (C&A) of NASA systems in 2007, implementation of the continuous monitoring program and the subsequent upgrade from red to yellow in status and from yellow to green on progress on the eGov scorecard by the Office of Management and Budget (OMB) serves as validation that significant and continuous progress is being made in the area of IT security.

DISCUSSION

1. IT security is not independent of IT management, but is one of the many components that comprise IT management. The infrastructure integration projects are a pervasive and wide-reaching conglomeration of initiatives that have a profound impact on IT security. The types of initiatives are inclusive of every possible security principle and associated service such as authentication (standardization and consolidation of SecurID tokens), access control (building out the NASA demilitarization zones (DMZ)), asset management, data encryption (at rest and in motion), configuration management (standard desktop configuration, vulnerability and patch management). While this is not an exhaustive list, the initiatives promote the security defense-in-depth model, which greatly enhances the Agency's security posture.

2. In September of 2007, the OCIO stood up the IT Security Program Management Office (ITS PMO) as a mechanism to assess the security posture of the organization, manage the human and financial capital, assess, modify and execute the CAP and monitor, create and overlay a security program management plan, which include the Agency's mission assets, and assess and reorganize all security projects under the ITS PMO's purview. The ITS PMO is fully functional and has aggressively engaged all of these activities making consistent, incremental and measured progress. Many of the MW deficiency milestones are either completed or are being improved upon. The ITS PMO is strengthening IT security policy NPR 2810.1x, adding organizationally defined control enhancements, created the three most critical standard operating procedures (SOP) with plans to enhance, improve and consolidate other SOPs, worked with the Agency procurement officer to simplify the IT security clause, established a new authoritative repository for creation and storage of enterprise system security plans (SSPs) and included a module for storing and reporting plan of action and milestones (POA&M).

In measuring the effectiveness of the program, the IT PMO has implemented a metrics program. Currently, the program measures different aspects of incident management, patch management and provides details on the status of implementing FISMA required activities. The results of these metrics are presented on a monthly basis to all the NASA CIOs for action. The metrics are also used to help identify and respond to systemic weaknesses that may reside within the agency-wide IT security program.

Furthermore, in 2007, NASA completed C&A for all NASA systems. This effort garnered the attention of OMB and in conjunction with progress made in other infrastructure and IT management initiatives, subsequently paved the way to an upgrade from red to yellow in status and from yellow to green on progress on the eGov scorecard by the Office of Management and Budget (OMB). This serves as validation that significant and continuous progress is being made in the area of IT security and IT management.

3. For a number of years, the Agency has suffered from an uncharacteristically large number of intrusions. The OIG has consistently noted that these intrusions are enabled by inconsistent management, operation and monitoring of IT resources. Compounding this has been the ineffective manner, in which the Agency has prepared for, detected and responded to, handle and reported incidents. It is the position of OCIO that the enterprise-wide Security Operations Center (SOC) implementation project is an effective mitigation strategy that will significantly improve the Agency's incident management program. Great strides have been taken in standing up the SOC implementation project and the Agency expects to begin showing incremental improvements to the incident management program over the next 6-12 months.

As part of the communications plan, the SOC implementation project team created a portal where project status and other information can be access by interested parties. This portal can be accessed by navigating to the following URL https://portal.nasa.gov/sites/arc/cio/projects/soc/status/default.aspx. It is the expectation of the Agency that this project remediate many of the incident response process and technology issues articulated by the OIG in its statement on material weaknesses issued in November 2006.

4. The ITS PMO has implemented a threat and situational awareness and mitigation program to proactively discover and handle sensitive intrusions into NASA's cyber assets. In partnership with the Office of Security and Program Protection (OSPP), the OCIO investigates for signs of intrusions into NASA's most critical assets. The Threat Identification Program (TIP), Cyber Threat Analysis Reporting (CTAR), and Advanced Incident Analysis (AIA) activities have been combined to create the Cyber Threat Analysis Program (CTAP). The program has proven to be a high yield activity and has gleaned tremendous support from the Department of Defense and members of the Intelligence Community. The CTAP program has briefed its findings to NASA's most senior leadership and at the request of the NASA Administrator to members of the Space Community.

DECISION

The Office of the Chief Information Officer, having shown demonstrable commitment to improving the security posture of the Agency through the execution of enterprise infrastructure improvements and progress against the IT security corrective action plan; and by adequately meeting the requirements of the Federal Information Security Management Act, is of the opinion that the IT security *material weakness* (MW) is disposed and makes declaration that the Agency's IT security posture can be classified as *other weakness* as defined by internal controls deficiencies classification.

The Agency believes that certain minimal conditions must exist in order to maintain or remove the OW classification. These conditions are:

- Continuous and substantiated progress must be made with regard to the CAP
- Visibility into the security posture of the mission assets must be achieved through the implementation of the enterprise SOC and regularly schedule compliance reviews.

AUTHORITY
Pursuant to the Federal Information Security Management Act (FISMA) § 3544(a) (3) (A).

Jerry L. Davis

cc:
Jonathan Pettus, Chief Information Officer
Bobby German, Deputy Chief Information Officer